



# SIMM 59

## Social Media Standard

[Also in 5320-S3 Acceptable Use Standard]

DRAFT

Revision 15 - December 16, 2009

CONFIDENTIAL

## Introduction

---

Agencies<sup>1</sup> and departments are encouraged to use Social Media technologies to engage their customers where appropriate. Many state entities, including the Governor's office, have used Social Media communication with great success, but as with most technologies, there is a measure of risk to address and mitigate. The following requirements will assist in risk mitigation.

This standard is not to be misinterpreted as requiring any state agency to allow the use of Social Media technologies in its environment. Further, this standard does not supersede any existing state agency Social Media policy which exceeds the requirements of this standard.

## General Requirements

---

### Agency Management Requirements

Prior to authorizing and enabling Internet access to Social Media websites, agency management shall:

1. Conduct a formal risk assessment of the proposed connections utilizing agency Risk Management processes. The assessment shall, at a minimum, include:
  - a. Analysis of the risks (including risk mitigation strategies) involved in providing Users access to Social Media websites including:
    - i. Employee productivity;
    - ii. Network bandwidth requirements and impacts;
    - iii. Reputational risk to personnel, the agency, and the State;
    - iv. Potential avenue for exposure or leakage of sensitive or protected information such as copyrighted material, intellectual property, personally identifying information, etc; and
    - v. Potential avenue for malware introduction into the organization's IT environment.
    - vi. The potential use of "other than government" sections of Social Media websites.
  - b. A cost/benefit analysis documenting the business need versus the technological, operational and administrative costs involved. These costs must include:

---

<sup>1</sup> When capitalized, the term "Agency" refers to one of the state's super Agencies such as the State and Consumer Services Agency or the Health and Human Services Agency. When used in lower case, the term "agency" refers to any office, department, board, bureau, commission or other organizational entity within state government. Within this standard, "agency" and "department" are used interchangeably.

- i. Staffing required to review content before it is posted;
- ii. Staffing required to monitor the Social Media websites for compliance;
- iii. Technology expenditures for upgrades or new software utilized by the Social Media websites, i.e., browsers, plug-ins, media players, etc.; and
- iv. Administrative costs in developing, implementing, and maintaining the policies and processes required below.

State agencies shall document this risk analysis and retain it for a minimum of two years following the termination of the Internet access to Social Media websites.

2. Ensure that agency policies and processes with sufficient staffing are in place to:
  - a. Approve Users based on business need to access the sites;
  - b. Determine the appropriate scope of connectivity, i.e., limiting to only government sections of the Social Media websites; and
  - c. On an ongoing basis, monitor all Social Media websites enabled for connection by agency personnel for compliance with this policy.
3. Formally document management's acceptance, mitigation, and handling of the risks involved, and retain it for a minimum of two years following the termination of the Internet access to Social Media websites.

## Agency IT Administrator Requirements

Agency IT Administrators shall:

1. Disable Internet access to Social Media websites from within the State Information Technology infrastructure until authorized by agency management after the requirements above have been met.
2. Disable Internet access to Social Media websites from within the State Information Technology infrastructure unless all Users' outbound connections are authenticated, tracked and filtered.
3. Limit Internet access Social Media websites to the greatest extent possible while allowing authorized Users to reach content necessary to fulfill the business requirements. Limitations may include:
  - a. Opening Internet access only to the government sub-domains on the Social Media websites;
  - b. Allowing Internet access to Users who are specifically authorized;
  - c. Preventing unnecessary functionality within Social Media websites, such as instant messaging (IM) or file exchange;

- d. Minimizing and/or eliminating the addition of web links to other websites, such as “friends”, to minimize the risk of exposing a government User to a link that leads to inappropriate or unauthorized material.
4. Enable technical risk mitigation controls to the extent possible. These controls may include:
  - a. Filtering and monitoring of all Social Media web site content posted and/or viewed
  - b. Scanning any and all files exchanged with the Social Media websites
5. At least annually, analyze the business need for, and benefits received from, continuing Internet access to Social Media websites, analyze the authorized Users with access to these Social Media websites to ensure compliance with the User Requirements (below), and document the results. Retain the analysis for a minimum of two years.

## User Requirements

1. Users shall connect to, and exchange information with, only those Social Media websites that have been authorized by agency management in accordance with the requirements within this and other agency and State policies.
2. Users shall minimize their use of “other than government” sections of the Social Media websites.
3. Users shall not post or release proprietary, confidential, sensitive, personally identifiable information (PII), or other state government Intellectual Property on Social Media websites.
4. Users who connect to Social Media websites through State information assets, who speak officially on behalf of the state agency or the State, or who may be perceived as speaking on behalf of an agency or the State, are subject to all agency and State requirements addressing prohibited or inappropriate behavior in the workplace, including acceptable use policies, User agreements, sexual harassment policies, etc.
5. Users shall not speak in Social Media websites or other on-line forums on behalf of an agency, unless specifically authorized by the agency head or the agency’s Public Information Office. Users may not speak on behalf of the State unless specifically authorized by the Governor.
6. Users who are authorized to speak on behalf of the agency or State shall identify themselves by: 1) Full Name; 2) Title; 3) Agency; and 4) Contact Information, when posting or exchanging information on Social Media

forums, and shall address issues only within the scope of their specific authorization.

7. Users who are not authorized to speak on behalf of the agency or State shall clarify that the information is being presented on their own behalf and that it does not represent the position of the State or an agency.
8. Users shall not utilize tools or techniques to spoof, masquerade, or assume any identity or credentials except for legitimate law enforcement purposes, or for other legitimate State purposes as defined in agency policy.
9. Users shall avoid mixing their professional information with their personal information.
10. Users shall not use their work password on Social Media websites.